Quelques exemples de technologies sans fil

équipe Planète - INRIA Rhône-Alpes
vincent.roca@inrialpes.fr
16 janvier 2009

Vue d'ensemble

- Deux aspects sont couverts :

1. **technologies IEEE-802.11* (Wifi)**
2. diffusion à grande échelle de contenus dans les réseaux DVB-H et UMTS
3. réseaux LTE de la 4G

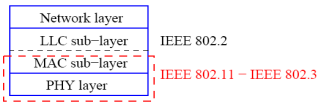
Partie 1:

Les réseaux sans fils IEEE-802.11/ WiFi

Nombreux transparents inspirés/empruntés à Imad Aad. Merci…

Introduction au IEEE 802.11/Wifi

- IEEE 802.11 et Wifi
  - ***IEEE 802.11* (*ISO/IEC 8802-11*) est un standard international décrivant les caractéristiques d'un réseau local sans fil (*WLAN*)**
  - **WiFi (*Wireless Fidelity*) est le nom donnée à la certification délivrée par la « Wifi Alliance », l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage (et marketing), le nom de la norme et de la certification sont confondus…**
- norme qui couvre les couches PHY / MAC



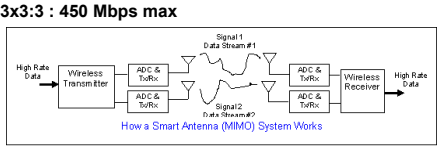
Introduction au IEEE 802.11/Wifi… (suite)

- les évolutions de la technologie :
  - 1997 802.11, 2 Mbps, autour de 2.4 GHz
  - 1999 802.11**b**, 11 Mbps, autour de 2.4 GHz
  - 1999 802.11**a**, 54 Mbps (25 Mbps utiles), autour **5 GHz**
  - 2001 802.11**g**, 54 Mbps (25 Mbps utiles), autour de 2.4 GHz, compatibilité ascendante avec 802.11b
- et quelques extensions :
  - 802.11e extension visant à apporter de la QoS
  - 802.11i extension visant à améliorer la sécurité de 802.11a/b/g

Introduction au IEEE 802.11/Wifi… (suite)

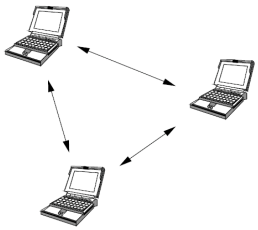
- nouvelle norme (9/2009) : 802.11n

  - jusqu'à 600 Mbps, autour de 2.4GHz ou 5GHz
  - rendu possible par :
    - **MIMO (mult input/mult output), via des antennes multiples**
    - **jusqu'à 4 flux simultanés**
    - **doublement de la bande passante des canaux (40MHz)**
    - **agrégation des trames**
  - configurations courantes :
    - **2x2:2, 2x3:2, 3x3:2 : 300 Mbps max**
    - **3x3:3 : 450 Mbps max**



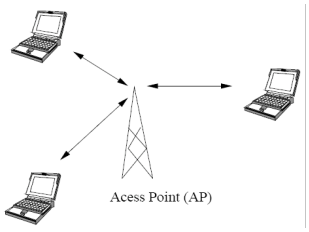
Les 3 modes de fonctionnement de 802.11

- le mode ad-hoc (ou IBSS, Independant Basic Service Set)
  - pas d'infrastructure fixe
  - interconnexion directe entre les équipements



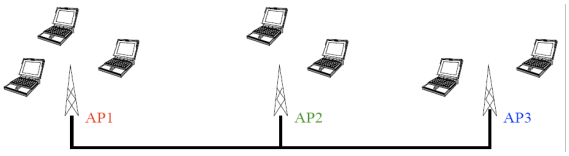
Les 3 modes de fonctionnement… (suite)

- le mode infrastructure basic (BSS, Basic Service Set)
  - présence d'un point d'accès qui peut aussi permettre l'interconnexion à l'Internet
  - pas de communication directe entre les équipements



Les 3 modes de fonctionnement… (suite)

- le mode infrastructure étendu (ESS, Extended Service Set)
  - présence de plusieurs points d'accès qui peuvent aussi permettre l'interconnexion à l'Internet
  - hand-off au niveau MAC entre les différents points d'accès
    - **la mobilité est transparente aux couches supérieures !**



Connexion au réseau

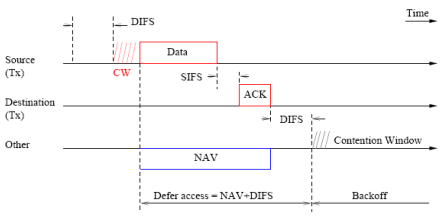
- Connexion passive
  - la station écoute sur tous les canaux les trames balises (***beacon frame***) émises par la BS
  - on obtient la liste des réseaux, avec leurs caractéristiques et le rapport S/N
- Authentification
  - la station s'authentifie auprès de la BS choisie
    - **peut être implicite, toute station étant acceptée**
    - **peut être explicite (Shared Key Auth. System) ⇒ nécessite une clef secrète partagée**
- Association
  - la station envoie une trame ***"association request"***
  - la BS vérifie le SSID spécifié et accepte si OK avec une trame ***"association response"***

La couche MAC

- Deux modes principaux
  - **DCF (Distributed Coordinated Function)**
    - **en mode Ad-Hoc ou Infrastructure**
    - **version de base pour les *petits* paquets**
    - **version permettant le CSMA/CA (Collision Avoidance) pour les autres paquets**
  - **PCF (Polling Coordination Function)**
    - **seulement en mode Infrastructure (puisqu'il faut un arbitre)**
    - **permet de garantir à chaque station un accès minimum au médium (absence de famine)**

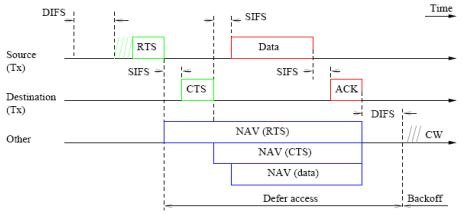
La couche MAC… (suite)

- Mode DCF, pour les petits paquets
  - introduit des temps d'attente minimums (DIFS/SIFS)
  - des temps d'attente aléatoires, bornés par une valeur qui dépend de l'historique (CW)
    - **la borne maximum augmente s'il y a collision…**



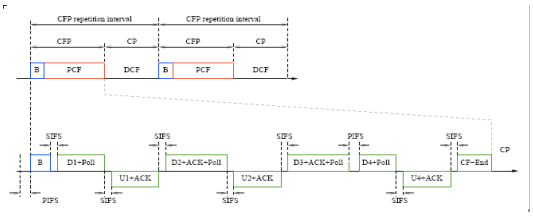
La couche MAC… (suite)

- Mode DCF avec Collision Avoidance
  - les RTS (Request To Send)/CTS (Clear To Send) suivent la même approche
  - les paquets (de taille conséquente) ne peuvent être transmis qu'après réception du CTS



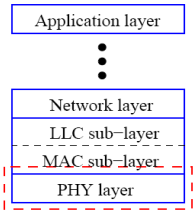
La couche MAC… (suite)

- Mode PCF pour garantir un accès minimum au médium (sans famine)
  - deux phases :
    - **polling, où le point d'accès interroge chaque station**
    - **DCF, où le système évolue librement sans intervention du point d'accès**



La couche physique de IEEE 802.11 (1997)

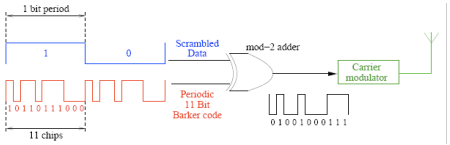
- 3 possibilités prévues par 802.11 - norme 1997
  - DSSS / FHSS / Infrarouge
  - mais essentiellement DSSS (étalement de spectre) en pratique



3 PHY types:
- DSSS (most products)
- FHSS (less products)
- IR (unknown products)

La couche physique de 1997… (suite)

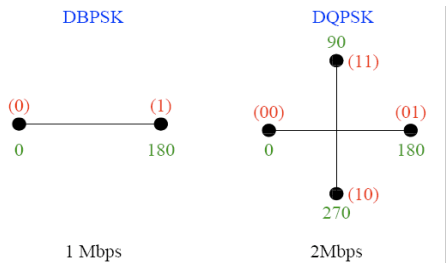
- Principe équivalent au DSSS présenté dans le cours sur la couche MAC…



- … mais avec des différences pratiques
  - un seul code de 11 bits partagé par tous les équipements
    - **n'apporte aucune sécurité**
    - **n'apporte aucun multiplexage d'accès**
    - **permet seulement la *suppression des interférences***

La couche physique de 1997… (suite)

- Deux types de modulations, suivant le débit souhaité et la robustesse



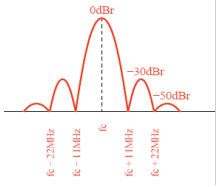
La couche physique du IEEE 802.11g

- Repose sur OFDM
  - un canal de 20 MHz est découpé en 52 sous-canaux
  - 48 sous-canaux pour les données, 4 pour des codes correcteurs
  - la modulation sur chaque sous canal est indépendante et bas débit
  - les 54 Mbps sont obtenus en aggrégeant ces sous-canaux

La couche physique… (suite)

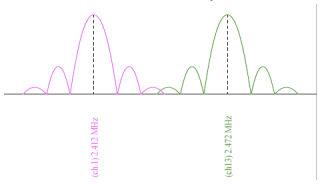
- les canaux possibles
  - **83,5 MHz de largeur de bande (2,4 à 2,4835 GHz)**
  - **14 canaux de largeur 20 MHz recouvrants**
  - **conduit à des recouvrements inévitables**

- le spectre de puissance
  - **de la largeur du canal en ignorant les lobes secondaires**



La couche physique… (suite)

- les canaux possibles : stratégie
  - en France, l'ACERP autorise les canaux de 1 à 13
  - en pratique, pour déployer un Wifi dans un site disposant déjà de réseaux Wifi :
    - **essayer d'éloigner les canaux le plus possible pour permettre un S/N élevé**
    - **sinon il y aura recouvrement et interférences donc débit plus faible (tout en continuant de fonctionner)**



La couche physique… (suite)

- Puissance de transmission

	GSM	802.11 (1997)
typique	100 – 600 mW	2.5 mW
maximum		100 mW

Wifi et sécurité

- Plusieurs mécanismes plus ou moins fiables...
- SSID
  - habituellement envoyé en clair dans les trames balises, on peut configurer la BS pour ne pas le faire
  - empêche une station de se connecter...
    - **... tant qu'elle n'a pas pu sniffer la connexion d'une station autorisée car le SSID est transmis en clair à ce moment là**

- *Access* Control List (ACL)
  - on liste sur la BS les adresses MAC autorisées
  - marche...
    - **... sauf si on sniffe des trames autorisées, et on change l'adresse MAC de sa carte (possible avec certaines cartes)**

Wifi et sécurité... (suite)

- WEP
  - permet une authentification et chiffrement
  - repose sur RC4 et une clef secrète partagée par BS et chaque station
  - marche bien...
    - **... tant que l'on n'a pas affaire à des attaquants un tout petit peu décidés**
    - **RC4 a bien des failles**
    - **les détails d'utilisation montrent qu'il y a des lacunes**
    - **on casse le tout après récupération d'un certain volume de trafic**

Wifi et sécurité... (suite)

- 802.11i
  - EAP (Extended Auth. Prot.) gère l'authentification
    - **inclue un contrôleur et un serveur d'authentification**
    - **plusieurs déclinaisons : par ex. EAP-TLS**
  - TKIP (Temporal Key Integrity Protocol)
    - **apporte chiffrement et intégrité**
    - **gère des clefs temporaires**
    - **indépendant du bloc de chiffrement : par ex. AES**
  - à utiliser impérativement !